Algorithmique de base

Master 1, Université de Rennes

10/10/2024 – TD 6

Exercise 1. Apply the Karatsuba algorithm to multiply the following two polynomials with coefficients in $\mathbb{Q}$:

$$f = x^4 + 3x^2 + 2x + 1, \quad \text{and} \quad g = 3x^3 + x + 2.$$

Exercise 2. Let ω be a primitive or principal n-th root of unity in a ring R. Show that

1. ω is invertible and ω^{-1} is also a principal or primitive n-th root of unity.
2. Let p, q be two distinct prime numbers. If $n = pq$ then ω^p is a q-th root of unity of the same nature as ω.
3. For $\ell \in \{1, \dots, n-1\}$, if ω is principal, we have

$$\sum_{j=0}^{n-1} \omega^{\ell j} = 0.$$

Exercise 3. Let $\mathbb{F}_q$ be the finite field with cardinality q. We want to show that $\mathbb{F}_q^* = (\mathbb{F}_q \setminus \{0\}, \cdot)$ is a cyclic group.

1. Show that the order d of an element of $\mathbb{F}_q^*$ divides $q-1$.
2. Show that $\mathbb{F}_q^*$ as at most d elements of order d.
3. Let $\alpha \in \mathbb{F}_q^*$ be an element of order d. Let H be the subgroup generated by α. Show that H is isomorphic to $\mathbb{Z}/d\mathbb{Z}$ and all the elements of order d are contained in H.
4. Show that $\mathbb{F}_q^*$ is cyclic.

Exercise 4.

1. Show that if n divides $q-1$ and α is a primitive element of $\mathbb{F}_q$ (i.e. α generates the multiplicative group $\mathbb{F}_q^*$) then $\alpha^{(q-1)/n}$ is a primitive n-th root of unity.
2. Let $\mathbb{F}_q$ be the finite field with cardinality q and let n be an integer. Show that $\mathbb{F}_q$ has primitive n-th root of unity if and only if $n|q-1$.

Exercise 5. Consider the field $\mathbb{F}_{17}$ and consider the following two polynomials in $\mathbb{F}_{17}[x]$:

$$f(x) = 5x^3 + 3x^2 - 4x + 3, \qquad g(x) = 2x^3 - 5x^2 + 7x - 2.$$

We want to compute $h = fg$ using the Fast Fourier transform algorithm. Since h will be of degree 6, we choose the nearest power of 2, that is $2^3 = 8$. So we fix $n = 8$ for the rest of the exercise.

1. Find a primitive 8-th root of unity ω in $\mathbb{F}_{17}$.
2. Calculate, using the DFT, the Discrete Fourier transform for ω, the evaluations of the polynomials f and g in $1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7$. Then compute the evaluations of fg in the powers of ω.
3. Compute ω^{-1} in $\mathbb{F}_{17}$.
4. Compute, using DFT, the constant coefficient and the coefficient of x^4 of h.
5. Compare the results with the product obtained by hand.
